SiVa ja SiGa teenused

AARE NURM

25.04.2019

Agenda

SiVa ja SiGa teenuste tutvustus ja nende liideste ülevaade

1. SiVa teenus
    I. Tutvustus
    II. Muudatused
2. SiGa teenus
    I. Tutvustus
    II. Liitumine
    III. Liides

SiVa – Signature Validation service

- Teenus allkirjade valideerimiseks. Võimaldab valideerida nii Eesti praeguseid, kui ajaloolisi formaate ning euroopa standardseid allkirja formaate (XAdES, PAdES, CAdES).
- Teenuse kirjeldus leitav: https://www.ria.ee/et/riigi-infosusteem/eid/partnerile.html#siva
- Tarkvara tehniline kirjeldus on leitav: http://open-eid.github.io/SiVa/
- Tarkvara leitav: https://github.com/open-eid/siva

SiVa V3 muudatused

- Simple raporti täiendused
- Ilma andmefailideta XAdES allkirjade valideerimine
- Diagnostic raport

Simple raporti täiendused

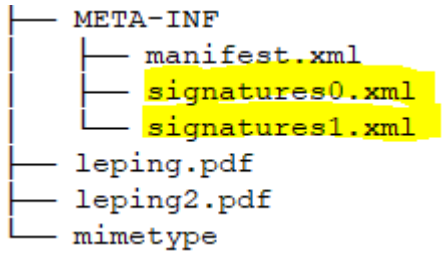
- Raportile on lisatud **subjectDistinguishedName** väli mis sisaldab **commonName** ja **serialNumber** välju. See võimaldab välismaalaste paremat tuvastamist.


```
"signatures": [{
    "signatureFormat": "XAdES_BASELINE_LT_TM",
    "subjectDistinguishedName": {
        "commonName": "JÕEORG,JAAK-KRISTJAN, 38001085718",
        "serialNumber": "PNOEE-38001085718"
    },
    "signedBy": "JÕEORG,JAAK-KRISTJAN, 38001085718",
```

Ilma andmefailideta XAdES allkirjade valideerimine

- Lisatud võimalus valideerida allkirju ilma andmefailideta.
  - Saab valideerida allkirju mis katavad konfidentsiaalseid andmefaile.
  - Saab valideerida suurte andmefailidega allkirju (SiVa teenusel 10MB piirang konteineri suurusele).
  - Vajab liidestujalt kehtivuse kontrolliks lisategevusi!

- Teenusesse laetakse konteineris olevad allkirjafailid. Liidestuja peab käitlema konteinerit ja selles olevaid faile.



Valideerimine andmefailide hashidega (peamine)

Andmefailide hashi arvutamise algoritmi leidmine

- Tuleb lugeda signatures*.xml failis olevat infot.

```
<asic:XAdESSignatures xmlns:asic="http://uri.etsi.org/02918/v1.2.1#">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="id-aed579cf7ba27f95411beaa24232f32f">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512"/>
            <ds:Reference Id="r-id-1" URI="leping.pdf">
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>WRlczpSZXZvY2F0aW9uVmFsd/yGH0qlE0FGsmUB2N3oLuhA==</ds:DigestValue>
            </ds:Reference>
```

Valideerimine andmefailide hashidega (peamine)

- Allkirja failist loetud hash algoritmiga tuleb arvutada andmefaili hash
- Andmefaili nimi, hash algoritm ja hash tuleb saata SiVa teenusele koos allkirjafailiga

Valideerimine andmefailide hashidega (peamine)

POST https://<server url>/validateHashcode


```
{
	"signatureFiles": [
		{
			"signature": "PD94bWwgdmVyc2lvbj...",
			"dataFiles": [
				{
					"filename": "leping.pdf",
					"hashAlgo": "SHA256",
					"hash": "WRlczpSZXZvY2F0aW9uVmFsd..."
				},
				{
					"filename": "leping2.pdf",
					"hashAlgo": "SHA256",
					"hash": "WRlpzaF0F0sda2vaW9uVmFsd..."
				}
			]
		},
		{
			"signature": "PDadw4mVyc2lvbj...",
			"dataFiles": [
				{
					"filename": "leping.pdf",
					"hashAlgo": "SHA256",
					"hash": "WRlczpSZXZvY2F0aW9uVmFsd..."
				},
				{
					"filename": "leping2.pdf",
					"hashAlgo": "SHA256",
					"hash": "WRlpzaF0F0sda2vaW9uVmFsd..."
				}
			]
		}
	],
	"reportType": "Simple",
	"signaturePolicy": "POLv4"
}
```

Valideerimine järelkontrolliga (mitte soovitatud)

POST https://<server url>/validateHashcode

- SiVa teenusele saadetakse ainult allkirjafailid. Reaalsete andmefailide ja allkirjades kasutatud andmefailide kattuvus tuleb liidestujal teha järelkontrollina!

```
{
  "signatureFiles": [
    {
          "signature": "PD9094wskjd..."
        },
        {
          "signature": "AD9sa4wsfsd..."
        }
  ]
}
```

Valideerimine järelkontrolliga (mitte soovitatud)

Andmefailide hashi arvutamise algoritmi leidmine

- Hash ja hashi algoritm tuleb võtta valideerimisraportist


```
"signatures": [{
    "signatureFormat": "XAdES_BASELINE_LT_TM",
    "subjectDistinguishedName": {
        "commonName": "JÕEORG,JAAK-KRISTJAN,38001085718",
        "serialNumber": "PNOEE-38001085718"
    },
    "signedBy": "JÕEORG,JAAK-KRISTJAN,38001085718",
    "claimedSigningTime": "2018-10-16T11:42:55Z",
    "signatureLevel": "QESIG",
    "signatureScopes": [{
        "scope": "FULL",
        "name": "test.txt",
        "hashAlgo": "SHA256",
        "content": "Full document",
        "hash": "LYwvbZeMohcStfbeNsnTH6jpak+l2P+LAYjfuefBcbs="
    }],
    "id": "S1",
    "indication": "TOTAL-PASSED",
    "info": {"bestSignatureTime": "2018-10-16T11:43:16Z"}
}],
```

Valideerimine järelkontrolliga (mitte soovitatud)

Kohustuslik järelkontroll

- Valideerimisraportist saadud andmefaili nime ja hashi algoritmi põhjal tuleb arvutada antud andmefaili hash.
- Arvutad hash peab peab kattuma raportis tagastatud andmefaili hashiga.
- **NB!** Kui hash ei kattu tuleb antud allkiri kuulutada mittekehtivaks vaatamata sellele, et SiVA valideerimistulemus on raportis positiivne.

Diagnostic raport

- Lisandunud on kolmas valideerimisraporti tüüp „Diagnostic“
- Raport tagastatakse ainult andmefailidega euroopa formaatide valideerimisel
- Raport sisaldab detailsemat infot allkirja objektide kohta (usaldusahelad, sertifikaadid, ...).

Ajaplaan

- Teenus testkeskonnas katsetamiseks
  - https://siva-arendus.eesti.ee/V3
  - Mai algus
- Teenus tootestatud
  - https://siva.eesti.ee/V3
  - Mai teine pool

SiGa – Signature Gateway service

- Teenus konteinerite loomiseks, allkirjastamiseks ja valideerimiseks.
- Avaliku sektori e-teenustel võimalus saada allkirjastamisega seotud funktsionaalsus ühest kohast.
- Ei vaja lisalepinguid usaldusteenuste jaoks, üks liitumine RIA-ga (tulevikus võib moodustada ka ühtse paketi Riigi Autentimisteenusega).

- Teenuse kirjeldust veel saadaval ei ole.
- Tarkvara tehniline kirjeldus leitav siit: https://github.com/open-eid/SiGa/wiki

SiGa etapp I

- Hashcode-i põhine konteinerite käsitlus
  - Uute konteinerite loomine
  - Konteineritele allkirjade lisamine
  - Mobiil-ID-ga allkirjastamine
  - Välise vahendiga allkirjastamine (ID kaart, e-tempel)
  - Konteineri valideerimine

SiGa jätkuarendused

- Andmefailidega konteinerite loomine, allkirjastamine, valideerimine
- Smart-ID-ga allkirjastamine
- Allkirjade küsimine/eemaldamine
- Andmefailide lisamine/eemaldamine/küsimine
- **NB! Oodatud on liidestujate tagasiside!**

SiGa teenusega liitumine

- Teenusega liitumiseks saata vastav avaldus help@ria.ee
- Liitumise protsess ja avaldus saab olema RIA kodulehel peale teenusega liitumise avamist.
- Test keskkonnaga liitumine ning liidestumise testimine on eelduseks toodangkeskkonnaga liitumiseks.
- Liitumistaotluse rahuldamaisel väljastatakse unikaalne kasutajatunnus ning saladus
- Võimalik on teenusepõhine liitumine:
  - Amet
    - Teenus 1 – unikaalne tunnus ja saladus
    - Teenus 2 – unikaalne tunnus ja saladus

Ajaplaan

- Test keskkond liidestumiseks valmis mai esimeses pooles
  - Liidestumiseks vajalik info avaldatakse RIA kodulehel
- Toodangu keskkond liidestumiseks valmis juunist.

Ligipääs SiGa teenusele

- Igal liidestunud teenusel on unikaalne kasutajatunnus ning saladus
- Kõik SiGa teenusele saadetud päringud peavad olema „allkirjastatud“ antud saladusega
- Autentimise kirjeldus: https://github.com/open-eid/SiGa/wiki/Authorization

Kasutusvoode näited

- Peamiste kasutusvoode näited on leitavad siit: https://github.com/open-eid/SiGa/wiki/Hashcode-API-main-flows

Hashcode konteiner

- Hetkel on ainult toetatud hashcode konteinerite kasutus
- Hashcode konteineri kuju on sama DigiDocService teenuses kasutatuga
  - Juhul kui olete DigiDocService teenusega liitunud peaks konteineri konversiooni osa jääma samaks
- Konteineri konversiooni kohta leiab infot siit: https://github.com/open-eid/SiGa/wiki/Hashcode-container-form

Enne

```
├── META-INF
│   ├── manifest.xml
│   └── signatures0.xml
├── **file1.txt**
├── **File2.docx**
└── mimetype
```

Pärast

```
├── META-INF
│   ├── **hashcodes-sha256.xml**
│   ├── **hashcodes-sha512.xml**
│   ├── manifest.xml
│   └── signatures0.xml
└── mimetype
```

API ülevaade

- REST –il põhinev liides
- Masinloetaval kujul on liides kirjeldatud WADL vormingus
- API kirjeldus on leitav siit: https://github.com/open-eid/SiGa/wiki/Hashcode-API-description

Java näidisrakendus liidestumiseks

- Loodud on Javal põhinev näidisrakendus mis ilmestab vajalikke tegevusi.
- Rakenduse kood on leitav siit: https://github.com/open-eid/SiGa/tree/develop/siga-sample-application

- Testnumbrid Mobiil-ID testimiseks on leitavad siit: https://github.com/SK-EID/dds-documentation/wiki/Test-number-for-automated-testing-in-DEMO

Küsimused?